Headquarters
United States Army, Europe, and Seventh Army
United States Army Installation Management Agency
Europe Region Office
Heidelberg, Germany

Army in Europe
Supplement 1 to AR 25-1*

28 April 2006

Information Management

Army Knowledge Management and Information Technology

***This supplement supersedes AE Supplement 1 to AR 25-1, 26 August 2005.**

For the CG, USAREUR/7A:

JAMES C. BOOZER, SR.
Colonel, GS
Deputy Chief of Staff

Official:

GARY C. MILLER
Regional Chief Information Officer - Europe

Summary. This supplement prescribes policy and procedures for Army Knowledge Management and Information Technology in the Army in Europe.

Summary of Change. This supplement has been revised to clarify information assurance (IA) policy (paras 2-30, 5-2, and E-2).

Applicability. This supplement applies to all Army organizations in Europe (including USAREUR specialized commands (AE Reg 10-5, app A)) and all DOD or non-DOD organizations using Army in Europe networks.

Supplementation. Organizations will not supplement this supplement without USAREUR G6 (AEAIM-AP) approval.

Forms. This supplement prescribes AE Form 25-1A, AE Form 25-1D, AE Form 25-1E, AE Form 25-1F, AE Form 25-1G, AE Form 25-1H, AE Form 25-1J, AE Form 25-1K, and AE Form 25-1L. AE and higher level forms are available through the Army in Europe Publishing System (AEPUBS).

Records Management. Records created as a result of processes prescribed by this supplement must be identified, maintained, and disposed of according to AR 25-400-2. Record titles and descriptions are available on the Army Records Information Management System website at *https://www.arims.army.mil*.

Suggested Improvements. The proponent of this supplement is the USAREUR G6 (AEAIM-AP, DSN 370-4254). Users may suggest improvements to this supplement by sending DA Form 2028 to the USAREUR G6 (AEAIM-AP), Unit 29351, APO AE 09014-9351.

Distribution. C (AEPUBS).

AR 25-1, 15 July 2005, is supplemented as follows:

Table of Contents. Add the following to the chapter 2 list:

2-30. Other Army in Europe Responsibilities

Table of Contents. Add the following to the chapter 8 list:

8-9. Army in Europe Records Management Policy

Table of Contents. Add the following to the list of appendixes**:**

D. Army in Europe Information Management and Resources Acquisition Process
E. Army in Europe Networks

Paragraph 2-2e, The NETCOM/9th ASC. Add the following:

The 5th Signal Command, under the operational control of USAREUR, is the NETCOM/9th ASC organization that exercises TECHCON and configuration-management authority for Army in Europe voice and data networks. Additionally, 5th Signal Command, in support of IMA-EURO, provides IM services to Army organizations in the European theater.

Paragraph 2-14a, Assistant Chief of Staff for Installation Management. Add the following:

In the European theater, the Regional Chief Information Officer - Europe (RCIO-Europe) is—

(1) Assigned to the Office of the Deputy Chief of Staff, G6, HQ USAREUR/7A.

(2) The primary POC for IM and IT for IMA-EURO, IMA-EURO subordinate organizations (such as United States Army garrisons (USAGs)), and all non-USAREUR organizations in the European theater.

(3) The G6, IMA-EURO.

(4) The approval authority for all service level agreements (SLAs).

(5) Responsible for ensuring organizations in (2) above follow the processes in appendix D.

Paragraph 2-16s, MACOM Commanders. Add the following:

In the European theater, the USAREUR G6 is the CIO. The USAREUR G6 reports to the CG, USAREUR/7A, and is the primary POC for IM and IT for HQ USAREUR/7A, V Corps, 21st Theater Support Command, United States Army Southern European Task Force, Seventh United States Army Joint Multinational Training Command, 7th Army Reserve Command, 266th Finance Command, 1st Personnel Command, and the United States Army Contracting Command, Europe. The USAREUR G6 is also the CG, 5th Signal Command; and, as the CG, 5th Signal Command, reports to the CG, NETCOM/9th ASC.

Paragraph 2-26, Commanders or Directors of MSCs, Field Operating Agencies, DRUs, Separately Authorized Activities, Tenant, and Satellite Organizations. Add subparagraphs c and d as follows:

c. The IMA-EURO, through the United States Army BASOPS Maintenance Center - Europe (USBMC-E), will operate the command Technical Information Equipment Repair (TIER) III Information Management Equipment (IME) Maintenance Program. For assistance on TIER III maintenance procedures, see *https://www.iis.5sigcmd.army.mil/scia/*. IMOs may contact their servicing maintenance desk for information. The TIER III IME Maintenance Program applies to all IMA-EURO commands and is available to non-IMA-EURO units in the USAREUR area of responsibility (AOR) on a reimbursable basis.

d. 5th Signal Command signal battalions, known as supporting signal battalions (SSBs), will support USAGs and may provide support to more than one USAG. Because the SSB provides IM services and support to customers who may be spread across more than one USAG, the organization (including support personnel) will be structured to perform that mission effectively. SSBs will be local command, control, communications, computers and information management (C4IM) service-level managers (LCSLMs). The primary responsibility of the LCSLM is the management, oversight, and delivery of required C4IM services within the assigned AOR. The RCIO-Europe is the approval authority for all SLAs between SSBs and the communities they support.

Chapter 2, Responsibilities. Add paragraph 2-30 as follows:

2-30. OTHER ARMY IN EUROPE RESPONSIBILITIES

a. DCG/CofS, USAREUR/7A. The DCG/CofS, USAREUR/7A, is the approval authority for—

(1) Defense Red Switch Network telephones.

(2) Commercial integrated service digital network (ISDN) lines in the quarters of preferred subscriber service (PSS) customers according to paragraph 6-4g.

(3) Exceptions to policy in this supplement not delegated to the USAREUR G6.

b. HQ USAREUR/7A and IMA-EURO Staff Principals, and USAREUR MSC and USAG Commanders. HQ USAREUR/7A and IMA-EURO staff principals, and USAREUR MSC and USAG commanders will—

(1) Designate the following for their organizations on orders:

(a) An IMO.

(b) An IAM to perform responsibilities outlined in AR 25-2 and AE Supplement 1 to AR 25-2.

(c) A TCO and an alternate TCO to manage funds and monitor command programs for base communications (BASECOM) services, including Defense Switched Network - Europe (DSN-E) service, DSN “99” access, commercial telephones, and cell phones.

(2) As responsible functional proponents (FPs), coordinate the fielding of new information systems (ISs) with the USAREUR G6, appropriate LCSLM, and 5th Signal Command before fielding proposed systems. This applies to IS fieldings initiated in the Army in Europe and those directed by higher headquarters. FPs are responsible for—

(a) Early and continuing notification to the USAREUR G6 of proposed system fieldings.

(b) Accreditation according to the Defense Information Technology Security Certification and Accreditation Process (DITSCAP).

(c) Compliance with the Army in Europe Networthiness Certification Program process (app E, para E-1).

(3) Participate in Army in Europe Program Evaluation Group (PEG) and information management working group (IMWG) meetings.

(4) Comply with the policy and procedures in appendixes D and E.

c. USAREUR G3. In addition to the responsibilities in subparagraph b above, the USAREUR G3 will—

(1) Be the requirements validation and approval authority for cell phones used for contingency-support missions and exercises. See *https://www.us.army.mil/suite/folder/1047603* for more guidance. (**NOTE:** Persons who have not previously been granted access to the page will have to request access before they will be able to view any documents.)

(2) Control the issue, turn-in, and reuse of exercise cell phones used by HQ USAREUR/7A staff offices. See *https://www.us.army.mil/suite/folder/1047603* for more guidance. (**NOTE:** Persons who have not previously been granted access to the page will have to request access before they will be able to view any documents.)

(3) Be responsible for preserving operational records.

d. Judge Advocate (JA), USAREUR. In addition to the responsibilities in subparagraph b above, the USAREUR JA will evaluate the legal aspects of requests for commercial ISDN service in the quarters of key Army in Europe personnel.

e. Information Infrastructure Assistance Team. The Information Infrastructure Assistance Team (I2AT) is part of the Command, Control, Communications, Computers, and Information Support (C4IS) Division, Office of the Deputy Chief of Staff, G6, HQ USAREUR/7A. The I2AT will—

(1) Conduct annual information-infrastructure assessments of Army in Europe organizations connected to AE telecommunications networks. During these assessments, the I2AT will evaluate automation systems, data networks, compliance with IA standards, use of IT, and telecommunications.

(2) Develop and maintain assessment and assistance policy, checklists, and schedules; establish visit-notification procedures; provide after-action reports; and establish procedures for collecting lessons learned. The I2AT will also consolidate and analyze assessment results, identify systemic problems, and conduct follow-up assistance visits when required.

(3) Provide training and guidance to command assessment teams in the European theater, which will conduct annual assessments of subordinate units. These teams will—

(a) Provide the results of their assessments to the I2AT Program Manager no later than 30 days after each assessment.

(b) Conduct follow-up assistance visits if needed.

(c) Coordinate with appropriate functional proponents for necessary technical expertise.

(4) Assess theater compliance with HQDA and Army in Europe policy and guidance and will refine and update assessment areas as new technology evolves.

NOTE: More information on the I2AT is available at *https://www.dcsim.hqusareur.army.mil/i2at/*.

Paragraph 3-3a, Planning. Add subparagraph (4) as follows:

(4) The Information Management Strategic Plan (*https://www.aeaim.hqusareur.army.mil/strategicplan.doc*) is a 5-year planning document developed by the USAREUR G6 that includes the CG, USAREUR/7A, vision and command goals to achieve that vision.

Paragraph 3-3e, Execution of C4/IT Investments. Add subparagraphs (5) through (8) as follows:

(5) Army in Europe organizations and HQ USAREUR/7A staff offices will comply with the policy and procedures in appendix D and more detailed guidance on C4/IT acquisition at *https://www.us.army.mil/suite/folder/1047603*. (**NOTE:** Persons who have not previously been granted access to the page will have to request access before they will be able to view any documents.)

(6) Army in Europe organizations may use the Government purchase card (GPC) for IM and IT purchases for items that cost less than $2,500. Other uses of the GPC for IM or IT items are prohibited. Requests for a waiver to this limit must be sent to the USAREUR G6 or to the RCIO-Europe for approval before any purchase is made.

(7) All IT items must have an approved information management acquisition request (IMAR) before they are procured. The unit making the request must send the IMAR to the SSB network service center (NSC) for validation. The NSC will validate automation-system requirements (for example, desktop or laptop computers) for technical functionality, affix an IMAR number, and then send the IMAR to the funding organization's command group for approval. For communications-systems IMARs (for example, network devices), the NSC will send the IMAR to the USAREUR G6 for validation. The United States Army Contracting Command, Europe (USACCE), and the Small Computer Issue Activity (SCIA) will not complete contracts that do not have valid IMAR numbers. AE units must submit all IT hardware and software to SCIA for acquisition using the Army Small Computer Program contracts and blanket purchase agreements. AE units must submit IT service requirements to USACCE.

(8) Only personnel identified as an IMO or information assurance security officer (IASO), with an appointment letter on file with the USAREUR G6 are authorized to request IT equipment or software. Personnel who attempt to order hardware or software without having an appointment letter on file will have their request returned without action. It is the responsibility of an organizations commander (or equivalent) to ensure current letters of appointment are filed with the USAREUR G6. All appointment letters must be recertified at the start of each fiscal year.

Paragraph 3-4, Process Analysis and Business/Functional Process Improvement. Add subparagraph h as follows:

h. Army in Europe organizations considering significant IT investments should contact the USAREUR G6 (AEAIM-AP) for information and assistance in process analysis and improvement.

Paragraph 3-5, CIO Validation of Requirements. Add subparagraph c as follows:

c. In the Army in Europe, the USAREUR G6 and the RCIO-Europe validate all C2/IT requirements by reviewing appropriate requirements documents. Validation criteria will include—

(1) A statement that all materiel solutions must be JTA-A compliant.

(2) Evaluation of emerging technologies.

(3) Outcome-oriented performance measurements.

(4) Compliance with IA requirements.

(5) Evaluation of new or modified requirements against existing systems.

(6) A 3-year life-cycle replacement schedule.

(7) Compliance with the policy and procedures in appendix D.

Paragraph 3-6, IT Performance Measurements. Add subparagraph k as follows:

k. Quantity Determination. Each year at each Army in Europe installation, the SSB and the USAG commander must collect, compile, and report the data necessary to build the overall evaluation for each IT metric (command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) capabilities documented in common levels of service) reported to USAREUR and HQDA. The SSB and USAG IT metric managers (and their respective commanders) will determine the required quantity of each IT metric that is required for the installation to fully accomplish its power-projection, sustainment, or training mission at 100 percent. This requirement is called “full mission requirement.” (Tactical C4ISR capabilities are not measured or reported by this process.)

(1) The ratio of “current capabilities” to the “full mission requirement” results in a percentage rating for that particular IT metric. Weights and standards for individual installation metrics and attributes are set by the USAREUR CIO to adjust for their relative importance in meeting the IT support mission of an installation.

(2) The weight factors assigned to each metric allow their weighted scores to be rolled up into a “percentage” rating for each attribute reported. Similar weight factors allow “attributes” to roll up into a percentage rating for the IT “capability.”

(3) Compiled IT metrics data will be used to identify mission-capability shortfalls and determine the budgetary requirements and the allocation and utilization of available IT resources.

(4) The Army in Europe IT metrics POC in the Office of the Deputy Chief of Staff, G6, HQ USAREUR/7A, will validate IT metrics data submitted by the SSBs and USAGs and send the information to HQDA each year.

Paragraph 3-8, IM/IT Human Capital Management. Add the following after the first sentence:

The USAREUR G6 is the proponent for CP-34 in the European theater.

Paragraph 4-2a, Army Knowledge Enterprise Architecture (AKEA). Add the following:

The 5th Signal Command, as the NETCOM/9th ASC representative, is responsible for developing and maintaining enterprise systems architectures for the Army in Europe. The USAREUR G6 (AEAIM-A) is responsible for consolidating the systems architecture and operational architecture, and for reiterating the technical architecture of the JTA-A as it applies to the Army in Europe. HQ USAREUR/7A staff offices, USAREUR MSCs, and capability communities of interest (COIs) are responsible for developing and maintaining their own internal architecture product sets while informing and participating in Army in Europe architect-development teams.

Paragraph 5-2, Management Structure for Information Assurance. Add subparagraphs g and h as follows:

g. The USAREUR G6 will appoint the IAPM for the European theater. IAPM responsibilities and duties are in AR 25-2 and AE Supplement 1 to AR 25-2.

h. HQ USAREUR/7A and IMA-EURO staff principals, and USAREUR MSC and USAG commanders will implement their IA programs according to AR 25-2 and AE Supplement 1 to AR 25-2.

Paragraph 6-1a, Information Transmission Economy and System Discipline. Add subparagraphs (4) through (7) as follows:

(4) TCOs request monthly DSN "99" use reports for their assigned organizations from their servicing dial central offices (DCOs) and maintain a detailed cell-phone usage report on all cell phones assigned in their AOR.

(5) TCOs ensure all BASECOM requirements above base-level services are validated in the SLA between their organization and the SSB.

(6) Operators use the most cost-effective service available when placing calls to CONUS. When calling CONUS from the European theater, DSN operators may use commercial long-distance services for official calls that are not being made for C2 purposes. DSN operators will not transfer nonemergency morale calls to other operators for "off-netting" (transferring the call to a commercial line) if those calls result in fees being charged to the U.S. Government.

(7) Personnel follow the guidance at *https://www.us.army.mil/suite/folder/1047603*. (**NOTE:** Persons who have not previously been granted access to the page will have to request access before they will be able to view any documents.)

Paragraph 6-2e(4), Software Control. Add the following:

Organizational IMOs, IASOs, or system administrators are responsible for centrally managing and keeping the original software media (installation CDs or diskettes, certificates of authenticity) and approval, registration, warranty, and disposition records. These records must be available for review (for example, by the judge advocate, inspector general, software companies). No software may be installed on Army in Europe networks without written approval of the organizational IMO, IASO, or system administrator. "Army in Europe networks" include local area networks (LANs), departmental LANs, wireless-enabled portable electronic devices (PEDs), and standalone PCs. A copy of this approval must be kept with software records.

Paragraph 6-3, Network Operations (NETOPS). Add subparagraphs h through j as follows:

h. Connection to DISA Networks. In the European theater, the Army Network Operations and Security Center - Europe (ANOSC-E) is responsible for regional oversight of local data networks that are connected to DISA networks. These local networks include the LandWarNet (Unclas) for unclassified data and the LandWarNet (Class) for classified data.

i. **LAN Administration and Network Management. S**upporting SSBs are responsible for LAN administration and network management.

j. Remote Access. The AE remote-access request forms (categories 1 and 2) will be used by personnel in Europe to request remote access to the Army in Europe LandWarNet (Unclas). (See paragraph E-5 for more information.)

(1) The category 1 form (AE Form 25-1H) will be used by DOD military personnel, DOD civilian employees, and permanently hired contractor personnel assigned to DOD agencies stationed in the European theater.

(2) The category 2 form (AE Form 25-1J) will be used by contractor personnel who are temporarily hired to accomplish specific official tasks that require remote access to the network.

(3) The forms must be completed by the requesting user, the unit IMO, and the approving authority (either a commander in the grade of O3 (for example, an Army captain) or higher, or a GS-13 or higher supervisor).

(4) Commanders approving remote access for their personnel must provide correctly configured Government-owned information systems (GOISs) for each user. AE Form 25-1K will be used to ensure correct equipment and configuration.

(5) The COR will also complete a portion of the category 2 form to validate that the requesting user is assigned to the contract and has an official requirement to remotely connect to the network.

(6) After the form has been completed and approved, the unit IMO will use it to complete an account request with the SSB.

(7) AR 25-400-2 requires that these forms be maintained in official unit files until the account is terminated or closed by the IMO in coordination with the SSB.

(8) Employee-owned information systems (EOISs) are not authorized to be used to remotely connect to the AE LandWarNet (Unclas).

Paragraph 6-4p, Video Teleconferencing (VTC). Add subparagraph (5) as follows:

(5) The USAREUR G6 is the approval authority for VTC systems and equipment. The 5th Signal Command operates and maintains VTC hubs in Europe and is responsible for developing and maintaining the VTC network architecture in Europe. The hubs provide multipoint VTC capability for secure C2 and common-user requirements. Certain VTC facilities are critical to the C2 of deployed forces. These facilities are directly connected to assigned ports on the secure VTC hub. Other VTC facilities will access the hub through commercial ISDN dial-up for the duration of scheduled VTCs.

(a) HQ USAREUR/7A and IMA-EURO staff principals and commanders of USAREUR commands and USAGs are responsible for—

1. Operating and maintaining internal VTC systems.

2. Registering H.320 and H.323 VTC systems with the Office of the Deputy Chief of Staff, G6, HQ USAREUR/7A.

3. Obtaining, loading, and initiating appropriate COMSEC keys for secure VTC.

(b) User-unit commanders will appoint a responsible and trained VTC operator and alternate as POCs for VTC operations.

(c) Requirements for garrison VTC systems, equipment, and facilities that cost more than the OPA threshold ($250,000) will be documented on DA Form 5695 and forwarded through IMO and SSB channels to the USAREUR G6 for forwarding to HQDA.

(d) More guidance is at *https://www.us.army.mil/suite/folder/1047603*. (**NOTE:** Persons who have not previously been granted access to the page will have to request access before they will be able to view any documents.)

Paragraph 6-4, Telecommunications System and Services. Add subparagraph ff as follows:

ff. AE-Unique Guidance. Additional guidance for telecommunication systems and services in the European theater is at *https://www.us.army.mil/suite/folder/1047603*. (**NOTE:** Persons who have not previously been granted access to the page will have to request access before they will be able to view any documents.) The guidance on that site applies to all Army and DOD organizations that use AE networks and must be used with the guidance in AR 25-1.

Paragraph 6-5f, The Defense Message System (DMS). Add subparagraph (3) as follows:

(3) Army in Europe guidance on DMS is at *https://www.us.army.mil/suite/folder/1047603*. (**NOTE:** Persons who have not previously been granted access to the page will have to request access before they will be able to view any documents.)

Paragraph 6-5, Long-Haul and Deployable Communications. Add subparagraph j as follows:

j. Requesting Long-Haul Services. Units that need long-haul commercial services must submit an RFS. DA Pamphlet 25-1-1 provides instructions for preparing RFSs. Additional guidance is at *https://www.us.army.mil/suite/folder/1047603*. (**NOTE:** Persons who have not previously been granted access to the page will have to request access before they will be able to view any documents.)

Paragraph 6-6, IT Support for Military Construction (MILCON). Add subparagraph e as follows:

e. Army in Europe guidance on MILCON is at *https://www.us.army.mil/suite/folder/1047603*. (**NOTE:** Persons who have not previously been granted access to the page will have to request access before they will be able to view any documents.)

Paragraph 7-2, Combat Camera (COMCAM). Add subparagraphs i through k as follows:

i. The Seventh United States Army Joint Multinational Training Command's Joint Multinational Readiness Center Vipers and Training Support Center in Vilseck will maintain COMCAM teams that are ready to deploy and provide COMCAM support when needed. These COMCAM teams will provide support for temporary emergency situations and only until relieved by the official military COMCAM team.

j. The Visual Information Services, Europe, will maintain, repair, or exchange COMCAM equipment as needed. This support may be augmented by civilian and military resources with the approval of the theater VI manager as required.

k. More guidance is at *https://www.us.army.mil/suite/folder/1047603*. (**NOTE:** Persons who have not previously been granted access to the page will have to request access before they will be able to view any documents.)

Paragraph 7-6, Automated Information Management System. Add the following:

Army in Europe VI activities will use the networking component of the VIAMS to the fullest extent possible. Subordinate DVIAN sites will provide appropriate site data required for reporting to the DVIAN holder. The DVIAN holder will consolidate all data into a single report for submission to the theater VI manager.

Paragraph 7-7c(2), Resourcing. Add subparagraph (e) as follows:

(e) Ergonomic requirements under host-nation law must be considered when purchasing and installing equipment. Systems will be installed to meet the ergonomic requirements of users.

Chapter 8, Records Management Policy. Add paragraph 8-9 as follows:

8-9. ARMY IN EUROPE RECORDS MANAGEMENT POLICY

a. AR 25-400-2 provides basic records management policy and procedures. AE Regulation 25-400-2 prescribes responsibilities, policy, and procedures for managing record information (paper and digital) in the European theater.

b. AR 25-55 prescribes policy and procedures for managing records under the Freedom of Information Act.

c. AR 340-21 prescribes policy and procedures for managing records under the Privacy Act.

Appendix A, section I, Required Publications. Add the following:

CJCSI 6740.01A, Military Telecommunications Agreements and Arrangements Between the United States and Regional Defense Organizations or Friendly Foreign Nations

DOD Directive 5000.1, The Defense Acquisition System

DOD Directive 8100.2, Use of Commercial Wireless Devices, Services and Technologies in the Department of Defense (DoD) Global Information Grid (GIG)

DISA-E Circular 310-140-2, Connection Approval Procedures (available at *https://www.eur.disa.mil/pubs/eurcirc.htm*) "Wireless Security Technical Implementation Guide" (published by the Defense Information Agency, available at *http://iase.disa.mil/stigs/index.html*)

USEUCOM Directive 100-1, USEUCOM Policy for Management and Protection of Theater Communications Networks

DA Pamphlet 25-1-1, Information Technology Support and Services

AE Supplement 1 to AR 25-2, Information Assurance

AE Regulation 10-5, HQ USAREUR/7A and Select Commands

AE Regulation 25-22, Use of U.S. Government Telecommunications Systems for Morale Purposes

AE Regulation 25-400-2, Army in Europe Record Information Management

USAREUR Regulation 604-1, Foreign National Screening Program (Laredo Leader)

Information Management Strategic Plan for Fiscal Years 2000 to 2004 (*https://www.aeaim.hqusareur.army.mil/strategicplan.doc*)

Appendix A, section II, Related Publications. Add the following:

AE Regulation 25-30**,** The Army in Europe Publishing Program

AE Regulation 25-35, Preparing Army in Europe Publications

USAREUR Regulation 25-10, American Forces Network Television-Europe

USAREUR Regulation 360-81, USAREUR Command Information Program

Appendix A, section III, Prescribed Forms. Add the following:

AE Form 25-1A, Request for Long-Term Loan or Purchase of Visual Information Equipment

AE Form 25-1D, Video Teleconferencing (VTC) Hub Registration

AE Form 25-1E, MCA User Requirements Checklist

AE Form 25-1F, Commercial Telephone Log/Report

AE Form 25-1G, Telephone Control-Number Log

AE Form 25-1H, AE LandWarNet Remote-Access Request-Category 1

AE Form 25-1J, AE LandWarNet Remote-Access Request-Category 2

AE Form 25-1K, AE Remote-Access Computer-Security Compliance Inspection

AE Form 25-1L, DMS/AMHS Organizational Account User Request

Glossary, section I, Abbreviations. Add the following:

AD	active directory
AE	Army in Europe
AMHS	Automated Message Handling System
ANOSC-E	Army Network Operations and Security Center - Europe
AOR	area of responsibility
BES	BlackBerry Enterprise Server
C&A	certification and accreditation
C4IM	command, control, communications, computers, and information management
CG, USAREUR/7A	Commanding General, United States Army, Europe, and Seventh Army
CIOEB	Chief Information Officer Executive Board
CPIC	Capital Planning and Investment Control
CTO	certificate to operate
DCG/CofS, USAREUR/7A	Deputy Commanding General/Chief of Staff, United States Army, Europe, and Seventh Army
DCO	dial central office
DISN-E	Defense Information Systems Network, Europe
DSN-E	Defense Switched Network - Europe
DUBOS	DSN Usage and BASECOM Ordering System
EOIS	employee-owned information system
FIPS	Federal Information Processing Standard
FP	functional proponent
FYDP	Future Year Defense Program
GOIS	Government-owned information system
GPC	Government purchase card
GSM	Global System Mobile
HQ USAREUR/7A	Headquarters, United States Army, Europe, and Seventh Army
I2AT	Information Infrastructure Assistance Team
IMA-EURO	United States Army Installation Management Agency, Europe Region Office
IMAR	information management acquisition request
IME	information management equipment
IMWG	information management working group
IPv6	Internet Protocol, version 6
IS	information system
ISDN	integrated service digital network
JA	Judge Advocate, USAREUR
LCSLM	local C4IM service-level manager
NETCOM/9th ASC	United States Army Network Enterprise Technology Command/9th Army Signal Command
NSC	network service center
OMA	Operations and Maintenance, Army
OPM	Office of Personnel Management
PBO	property book officer
PED	portable electronic device
PSS	preferred subscriber service
RCERT-E	Regional Computer Emergency Response Team, Europe

RCIO-Europe	Regional Chief Information Officer - Europe
S/MIME	secure/multipurpose Internet mail extension
SCIA	Small Computer Issue Activity
SES	Senior Executive Service
SIM	subscriber identity module
SOIC	senior official of the intelligence community
SSAA	system security accreditation agreement
SSB	supporting signal battalion
TCO	telephone control officer
TDY	temporary duty
TIER	technical information equipment repair
TSACS	Terminal Server Access Control System
UCMJ	Uniform Code of Military Justice
UMS	USAREUR metadata standard
USACCE	United States Army Contracting Command, Europe
USAG	United States Army garrison
USAREUR	United States Army, Europe
USBMC-E	Unites States Army BASOPS Maintenance Center - Europe
USEUCOM	United States European Command
VoIP	voice over Internet Protocol
VPN	Virtual Private Network

APPENDIX D
ARMY IN EUROPE INFORMATION MANAGEMENT AND RESOURCES ACQUISITION PROCESS

D-1. INFORMATION TECHNOLOGY INVESTMENT STRATEGY GUIDANCE

NOTE: This paragraph supplements guidance to AR 25-1, paragraphs 3-3b(1) through (5), which all organizations are responsible for following.

a. The Army in Europe Program Evaluation Group (PEG), co-chaired by the USAREUR G6 and Regional Chief Information Officer - Europe (RCIO-Europe), will—

(1) Oversee and review unique command, control, communications, computers, and information technology (C4/IT) initiatives.

(2) Validate ongoing system projects.

(3) Change project priorities as necessary.

b. All AE C4/IT special initiatives require PEG approval. After PEG review, C4/IT initiatives valued at $25,000 or more will be sent to the Army Chief Information Officer Executive Board (CIOEB). The CIOEB will review and concur or nonconcur in total on PEG recommendations for information technology (IT) investments.

c. The Army in Europe Information Management Working Group (IMWG) will evaluate and recommend to the PEG the prioritized IT requirements for the Army in Europe. The IMWG is responsible for establishing and maintaining the Army in Europe overall IT portfolio. The IMWG will meet at least once a quarter or more often if necessary. IMWG members are representatives from the following organizations:

(1) Office of the Deputy Chief of Staff, G1, HQ USAREUR/7A.

(2) Office of the Deputy Chief of Staff, G2, HQ USAREUR/7A.

(3) Office of the Deputy Chief of Staff, G3, HQ USAREUR/7A.

(4) Office of the Deputy Chief of Staff, G4, HQ USAREUR/7A.

(5) Office of the Deputy Chief of Staff, G6, HQ USAREUR/7A.

(6) Office of the Deputy Chief of Staff, G8, HQ USAREUR/7A.

(7) IMA-EURO.

(8) V Corps.

(9) United States Army Southern European Task Force.

(10) 21st Theater Support Command.

(11) Seventh United States Army Joint Multinational Training Command.

(12) 7th Army Reserve Command.

(13) 5th Signal Command.

(14) 1st Personnel Command.

(15) 266th Finance Command.

(16) United States Army Europe Regional Medical Command.

(17) United States Contracting Command, Europe.

d. Each organization's IMWG member in subparagraph c above will work with his or her local command, control, communications, computers, and information management (C4IM) senior managers to conduct a mission analysis before attending IMWG meetings. Mission analysis is a strong, forward-looking, and continuous analytical activity that evaluates the ability of the organization's assets to meet existing and emerging demands for services. Mission analysis enables the organization to determine and prioritize the most critical capability shortfalls and best technology opportunities for improving overall security, capacity, efficiency, and effectiveness in providing services to customers.

e. Each organization will prepare a preliminary budget estimate. The preliminary budget estimate should provide—

(1) Enough information to support detailed planning and concept development before investment selection.

(2) An order-of-magnitude estimate of budget requirements to support a Future Year Defense Program (FYDP) budget plan and life-cycle costing. Life-cycle replacement in the Army in Europe will be based on a 3-year cycle. This means that 33 percent of assets will be replaced each year.

f. Army in Europe investments will be made according to the Army in Europe Investment Strategy and the Army in Europe Capital Planning and Investment Control (CPIC) process. The CPIC process—

(1) Is a structured approach to managing IT investments. It ensures that all IT resources will meet mission and support-mission needs.

(2) Ensures IT investments are well thought out and cost-effective. This helps reduce risks and get the most from IT resources throughout their life cycle. The CPIC process includes the following phases:

(a) Pre-selection.

(b) Selection.

(c) Control.

(d) On-going evaluation.

(3) Is used to monitor proposed and ongoing projects and initiatives throughout their life cycle. Successful investments and those that are terminated or delayed are evaluated to assess their effect on future proposals and to benefit from any lessons learned.

(4) Involves completing one phase of the CPIC process ((2) above) before beginning the next phase. Senior decision-makers oversee each phase with the help of the appropriate community portfolio owner. This ensures that each investment receives the appropriate level of managerial review and that coordination and accountability exist.

(5) More guidance on the Army in Europe Investment Strategy process is at *https://www.us.army.mil/suite/folder/1047603*. (**NOTE:** Persons who have not previously been granted access to the page will have to request access before they will be able to view any documents.)

D-2. C4 SUPPORT TO U.S. MILITARY PERSONNEL SERVING IN NATO BILLETS

NOTE: This paragraph supplements guidance to AR 25-1, paragraphs 6-1 and 6-5, which all organizations are responsible for following.

a. Chairman, Joint Chiefs of Staff, Instruction (CJCSI) 6215.01B and CJCSI 6740.01A allow for command, control, communications, and computers (C4) support (including Defense Information Systems Network (DISN) and Defense Switched Network (DSN) services) to be provided to U.S. military personnel assigned to U.S. billets in international organizations (for example, NATO units) if the proper authorization for the support has been obtained.

b. Requests for C4 service require Joint Staff or higher approval. U.S. military personnel who need C4 service will submit requests for support through the USAREUR CIO to USEUCOM (ECJ6-S), Unit 30400, Box 1000, APO AE 09128-1000. On receipt of validation and approval from USEUCOM, the requesting organization will coordinate with the servicing supporting signal battalion (SSB) to meet the requirement.

c. The SSB will determine if it has the capability and resources to provide the requested service and will support the request when it can. If unable to provide the service, the SSB will send the request through technical channels to the USAREUR G6 (AEAIM-C), which will coordinate to provide the requested service.

d. If a service involves incremental Operations and Maintenance, Army (OMA), costs, the USAREUR G6 will coordinate with the USAREUR G8 (AEAGF-ND) to determine the availability of OMA BA 44 (Support of Other Nations) funds to support the service.

D-3. ARMY IN EUROPE SMALL COMPUTER ISSUE ACTIVITY (SCIA)

NOTE: This paragraph supplements guidance to AR 25-1, paragraphs 3-2d and 6-2i, which all organizations are responsible for following.

a. All IT items that are $2,500 or more will be purchased through the Small Computer Issue Activity (SCIA). Complete guidance on the SCIA process is at *https://www.iis.5sigcmd.army.mil/scia/*. Requests for exception to the requirement to purchase through SCIA must be sent to the RCIO-Europe or USAREUR G6 (AEAIM-A) for approval.

b. SCIA will only process IT procurements which have a valid, approved information management acquisition request (IMAR) number from the supporting network service center for automation requirements or the USAREUR CIO for communication requirements.

c. SCIA will maintain accountability of the IT request through life-cycle replacement and turn-in of the property.

D-4. MICROSOFT ENTERPRISE LICENSE AGREEMENT (ELA)

NOTE: This paragraph supplements guidance to AR 25-1, paragraphs 6-2a and 6-2e(3), which all organizations (except joint DOD organizations) are responsible for following.

a. The ELA is a 6-year contract between the Army and Microsoft Corporation. It was established to reduce the cost of Microsoft software to the Army and to support Army Knowledge Management (AKM) goals by standardizing the desktop configuration, deploying Active Directory (AD) technology, and managing the Army's IT infrastructure.

b. All Army in Europe units and organizations will—

(1) Follow ELA procedures for purchase of Microsoft software and product services.

(2) Fulfill the terms of any existing enterprise contracts with Microsoft before ordering software through the ELA.

(3) Maintain accountability of software received through the ELA. Commanders must ensure distribution does not exceed the quantities authorized on the license certificate.

(4) Allow only information management officers (IMOs) or information assurance security officers (IASOs) with valid appointment orders on file at the USAREUR G6 (AEAIM-A) to request software through the Army Small Computer Program (ASCP) website (*https://ascp.monmouth.army.mil*). The appointment orders must be signed by a commander in the grade of O5 or above. If, for reasons of exercise or deployment, the commander is not physically present, an appointed representative may sign the appointment order.

(5) Order new or life-cycle replacement server hardware without operating system software. Workstations must be ordered with a Microsoft Window XP operating system that includes only the DA CIO/G6 baseline. This requirement may be waived only by the RCIO-Europe for legacy platforms that support defined requirements.

(6) Use the ELA as their only source for Microsoft software products and services and will order only through the ASCP website (*https://ascp.monmouth.army.mil*).

c. The process to request and receive Microsoft products in the European theater will be accomplished as a coordinated effort between the United States Army Network Enterprise Technology Command/9th Army Signal Command (NETCOM/9th ASC); the ASCP; the Office of the Deputy Chief of Staff, G6, HQ USAREUR/7A; 5th Signal Command; and IMA-EURO organizations.

d. The Deputy USAREUR G6 and RCIO-Europe are the approval authorities for exceptions to this policy.

APPENDIX E
ARMY IN EUROPE NETWORKS

E-1. NETWORTHINESS CERTIFICATION PROGRAM

NOTE: This paragraph supplements guidance to AR 25-1, paragraph 6-3g, which all organizations are responsible for following.

a. The Army Networthiness Certification Program manages the specific risks associated with the fielding of information systems (ISs) and supporting efforts on the LandWarNet. The Army in Europe Certificate to Operate (CTO) Program is used to identify and manage USAREUR- and installation-level risks as required by the Army Networthiness Certification Program. Installation-level issues include the effect IS may have on the AE LandWarNet, life-cycle support, operations, maintenance and management plans, training, existing ISs, and local security. More information and implementation guidance on the Army in Europe CTO Program is at *https://www.us.army.mil/suite/folder/1047603*. (**NOTE:** Persons who have not previously been granted access to the page will have to request access before they will be able to view any documents.)

b. The Networthiness Certification Program applies to all organizations fielding, using, or managing an IS on the AE LandWarNet. Any IS operating without a networthiness certificate is subject to removal from the AE enterprise network.

c. The USAREUR G6 will—

(1) Provide policy for and oversee the Army in Europe CTO Program.

(2) Be the Army in Europe CTO program manager.

(3) Coordinate CTO staffing actions within the Army in Europe.

(4) Assist Army in Europe IS functional and program management offices obtain networthiness certification.

(5) Consolidate enterprise systems and operational architectures in the European theater.

d. The Regional Chief Information Officer - Europe (RCIO-Europe) will be the CTO approval authority.

e. The 5th Signal Command will—

(1) Serve as the CTO recommendation authority. Recommendations will be based on results of integrated logistics support, bandwidth, funding, and fielding analyses.

(2) Validate that the AE enterprise network can support ISs, that there are no negative effects to other ISs, that ISs do not introduce security vulnerabilities, and that ISs can be managed and maintained.

(3) Ensure that any IS operating on the AE enterprise network has an approved networthiness certification.

f. The Information Assurance Program Manager will—

(1) Validate the development of certification and accreditation (C&A) documentation by reviewing and endorsing such documentation and recommending action.

(2) Ensure ISs do not introduce security vulnerabilities.

(3) Make a CTO recommendation based on IA analysis.

g. Army in Europe organization and activity commanders, heads of organizations assigned or attached to Army in Europe organizations, and Army in Europe IS functional managers will—

(1) Ensure ISs have a networthiness certification before fielding.

(2) Request a networthiness certification for AE-developed or -sponsored IS from the USAREUR CTO Program Office.

E-2. WIRELESS IS AND PORTABLE ELECTRONIC DEVICES

NOTE: This paragraph supplements guidance to AR 25-1, paragraph 6-4c, which all organizations are responsible for following. The POC for information in this paragraph is the USAREUR G6 (AEAIM-C, DSN 370-7633). The policy on wireless IS and portable electronic devices is at *https://www.us.army.mil/suite/folder/5423602*. (**NOTE:** Persons who have not previously been granted access to the page will have to request access before they will be able to view any documents.)

E-3. BLACKBERRY DEVICES

NOTE: This paragraph supplements guidance to AR 25-1, paragraphs 6-2e(6) and 6-4, which all organizations are responsible for following. The POC for information in this paragraph is the USAREUR G6 (AEAIM-C, DSN 370-7633).

a. BlackBerry devices provide remote e-mail access to the LandWarNet (Unclas) to support official business. Because they are easy to use and tightly integrated with existing infrastructure, BlackBerry devices are authorized for personnel to allow encrypted, always-on access to e-mail. The infrastructure to support this technology will be implemented by the Army in Europe, but each organization will pay for its own devices and services. Personnel authorized to approve the acquisition of the BlackBerry devices (d below) must consider the overall long-term cost to their organizations before approving the acquisition. BlackBerry devices should be acquired only for personnel who require a mobile e-mail capability as a mission-critical tool.

b. BlackBerry systems used in the Army in Europe must be certified to meet the Federal Information Processing Standard (FIPS). FIPS certification protects unclassified Government information when leaving DOD-owned and -controlled networks. BlackBerry systems must use secure/multipurpose Internet mail extension (S/MIME) software to be Public Key Infrastructure (PKI) compliant. S/MIME-enhanced BlackBerry systems are subject to DOD, DA, and AE policy governing the security and use of unclassified ISs.

c. In addition to general security regulations and policy, the following controls govern the use of BlackBerry systems in the European theater:

(1) The use of BlackBerry handheld devices must be included in the using organization’s system security accreditation agreement (SSAA). The BlackBerry enterprise server (BES) must be included in the same SSAA as its host Microsoft exchange server.

(2) The BlackBerry handheld device will not be used to process classified information (Confidential and above). If the device is compromised beyond the ability of the internal S/MIME “purging” features to ensure that no data remains or if the device is damaged beyond in-house repair capabilities, the device must be destroyed according to applicable Army regulations.

(3) The BlackBerry handheld device will not be taken inside any permanent, temporary, or mobile sensitive compartmented information facility (SCIF) without approval of the senior official of the intelligence community (SOIC). Any infrared capability must be disabled before entering a SCIF. Although the device may be approved by the SOIC for use in a SCIF, the radio-frequency capability will not be used. This restriction may be waived only by the Special Security Officer, Defense Intelligence Agency (DAC-2A), and only if use of radio-frequency capability in a SCIF is mission essential.

(4) The BlackBerry handheld device will not be taken into areas where classified information is discussed or electronically processed except as provided for in (3) above or AR 25-2, paragraph 4-28. Users will receive security-awareness training.

(5) The BlackBerry handheld device will not be configured to work with or be connected to any device other than a Government-owned unclassified computer. Autoforwarding official mail (from a *.mil* e-mail address) to unofficial accounts (for example, a *.com* e-mail address) or unofficial devices is prohibited.

(6) The BlackBerry device will employ password protection for the device, the subscriber identity module (SIM) chip, and the handheld certificate store (handheld key store). Devices will be configured with a timeout of 15 minutes, a password history of five, and maximum password attempts of five. On the fifth failed attempt, all data on the device will be wiped automatically. Based on this password policy and the limitations of the device, passwords must be five alphanumeric characters with at least one alpha and one numeric character. BlackBerry passwords will be changed every 150 days.

(7) The cell-phone policy in paragraph E-10a applies to the "telephony capabilities" of the BlackBerry.

(8) Every BES must comply with the latest Army in Europe BlackBerry configuration (IT policy) requirements. (This configuration policy is available from the USAREUR G6 (AEAIM-AP) (DSN 370-7724)). BESs must have USAREUR G6 approval before being purchased or added to Army in Europe networks.

(9) If a BlackBerry handheld device is lost or stolen, it must be reported immediately to the BES administrator. The BES administrator will immediately issue a "kill" command for the device, wiping all data from it.

(10) Each BlackBerry has a unique hardware address known as a personal identification number (PIN). PIN-to-PIN messaging (sending messages between BlackBerries using the BlackBerry's PIN instead of e-mail addresses) is unencrypted and is not authorized. The USAREUR G6 may authorize PIN-to-PIN messaging for limited periods during critical situations when normal communication infrastructure is unavailable.

d. BlackBerry devices are pre-approved for general officers, Senior Executive Service (SES) civilian employees, promotable colonels, and for commanders and command sergeants major at the brigade level and above. BlackBerry devices are available in the USAREUR area of responsibility (AOR) for all personnel but must be approved at the assistant deputy chief of staff, HQ USAREUR/7A (colonel, GS-15, or higher), USAREUR major subordinate command commander level. This approval authority will not be delegated. Organizations and units subordinate to the IMA-EURO must request approval from the Director, IMA-EURO. Approval to purchase BlackBerry devices will be based on a valid requirement for mobile e-mail capability and granted only after considering the costs involved.

(1) BlackBerry devices will be purchased with the necessary service as part of the USAREUR cell-phone contract at the requesting unit's expense. No other contract source is authorized. Units are responsible for all costs for the device, licenses, monthly charges, and usage.

(2) BlackBerry devices will be used with the appropriate Common Access Card (CAC) sled. This will allow use of CAC certificates for PKI-enabled e-mail. Only the USAREUR G6 may approve exceptions to this rule.

(3) BlackBerry handheld devices must be maintained on property books. BlackBerry devices will remain with the unit when the user leaves the unit.

(4) Personnel are authorized only one cell-phone service contract (one subscriber identity module (SIM) chip) at a time, regardless of how many hardware devices they require or use. A BlackBerry user, for example, who also uses a secure or nonsecure cell phone must swap the single SIM chip between devices when required. Under no circumstances will users have more than one service contract.

e. Unless specifically stated otherwise, only the DCG/CofS, USAREUR/7A, may approve exceptions to this policy.

E-4. VOICE OVER INTERNET PROTOCOL (VoIP)

NOTE: This paragraph supplements guidance to AR 25-1, paragraph 6-5a, which all organizations are responsible for following. The POC for information in this paragraph is the USAREUR G6 (AEAIM-C, DSN 370-7633).

a. VoIP networks will not be used as the primary voice communications system. Organizations must maintain traditional DSN connectivity for all command and control requirements.

b. Approval from the USAREUR G6 is required before VoIP networks are procured, installed, or used to store, process, or transmit information. The VoIP request memorandum must be sent through the supporting NSC, the SSB, 2d Signal Brigade, 5th Signal Command, to the USAREUR G6. The USAREUR G6 will review the request and send a recommendation to approve or disapprove the request to the Defense Information Systems Agency (DISA). If approved, the VoIP network must be purchased at the requesting unit's expense. The VoIP system will not be approved until it receives an information assurance certification and accreditation (IACA) by the DISA designated accreditation authority (DAA). It will not be connected to or planned for connection to the Defense Switched Network (DSN) until the required approvals from USAREUR and DISA have been received by the unit.

c. VoIP systems must be compliant with overall network-security architecture and appropriate enclave security requirements. All VoIP devices must be added to the unit's SSAAs, and the complete VoIP network must have a valid networthiness certification before being connected to the LandWarNet.

d. VoIP traffic between employee-owned information systems (EOISs) and Army in Europe ISs is prohibited.

E-5. NETWORK REMOTE ACCESS

NOTE: This paragraph supplements guidance to AR 25-1, paragraph 6-5a, which all organizations are responsible for following. The POC for information in this paragraph is the USAREUR G6 (AEAIM-A, DSN 370-7577).

a. A “remote user” is a person who enters the AE LandWarNet (Unclas) from outside the physical or logical boundary of the internal local area network (LAN). The remote-access system creates a protected extension of the AE LandWarNet (Unclas) for authorized remote users. The LandWarNet (Unclas) remote-access system has the following components:

(1) Access to the network. Users will connect through either the Terminal Server Access Control System (TSACS) or a commercial Internet service provider (ISP) that provides dial-up, broadband, wireless, or leased-line services. TSACS and these other network connections provide unencrypted connections to the network.

(2) A Virtual Private Network (VPN). The primary function of VPN is to encrypt the path from the user to the network. VPN will allow remote users to—

(a) Protect Army information that is sent and received during remote communications with other users and servers on the AE LandWarNet (Unclas).

(b) Use the applications available to them in their normal office environment.

(c) More information and the USAREUR VPN client software are available at *https://www.anosce.5sigcmd.army.mil/index.php?option=com_content&task=view&id=248&ttemid=276.*

b. Remote access to the AE LandWarNet (Unclas) will be used only for unclassified official business. Remote access will never be used to process classified data. Remote users will be subject to monitoring; their connection will be terminated if it causes damage to any part of the network or if their computer is not configured correctly. Personnel who abuse or misuse remote-access capabilities may be disciplined in accordance with the Uniform Code of Military Justice (UCMJ) or Office of Personnel Management (OPM) directives and may have their remote-access account terminated.

c. The 5th Signal Command will—

(1) Manage all remote-access points.

(2) Configure all remote-access equipment to require authentication and encryption. VPN functionality on remote-access equipment is required.

d. Only commanders who are captains and above or supervisors in the grade of GS-13 and above may approve requests for remote access. These approval authorities will also be responsible for—

(1) Pre-approving reimbursement for temporary duty (TDY) or remote-access connection charges at the user’s home station.

(2) Setting specific limits when pre-approving reimbursement for connection charges ((1) above). Generally, home-station remote-access users should not be reimbursed, because they normally can return to their office.

(3) Paying approved reimbursements for remote-access charges with internal operations and maintenance (O&M) funds.

e. Information management officers (IMOs) will—

(1) Use the appropriate AE remote-access request form (AE Form 25-1H or AE Form 25-1K) to request approval for remote access with their supporting NSC.

(2) Keep completed forms ((1) above) in unit records and coordinate new and deleted accounts with the supporting NSC.

f. EOISs are prohibited from connecting to the Army network for any purpose. If the approving authority (d above) determines that a person has a need for remote-access, then that authority must provide a Government-owned information system (GOIS). IMOs and remote-access users will complete AE Form 25-1K to ensure the GOIS to be used for remote access is correctly configured.

E-6. INTERNET PROTOCOL, VERSION 6 (IPv6)

NOTE: This paragraph supplements guidance to AR 25-1, paragraph 6-3, which all organizations are responsible for following. The POC for information in this paragraph is the USAREUR G6 (AEAIM-A, DSN 370-7577).

All Army in Europe units will—

a. Appoint an IPv6 transition officer to coordinate the organization's transition to IPv6. Each USAREUR major subordinate command (MSC) and United States Army garrison (USAG) will send a copy of its appointment orders to the IPv6 Transition Office, 5th Signal Command, CMR 421, APO AE 09056-0421.

b. Plan for replacement and retirement of all IPv4 equipment and software before fiscal year 2008 as part of life-cycle replacement procurements. All automation equipment and software developed, procured, or acquired must be IPv6 compatible.

(1) Units will use the Small Computer Issue Activity (SCIA) when purchasing new IT systems to ensure they are IPv6 compatible.

(2) If a requested item is mission essential but not IPv6 compatible, there must be a request for exception to policy. The request for exception must justify the need for the non-IPv6-compatible system and explain the requesting unit's plan to transition to an IPv6-compatible system.

c. Transition to IPv6 will be accomplished only after coordinating with and receiving approval from 5th Signal Command. The 5th Signal Command will provide an implementation plan in coordination with the United States Army Network Enterprise Technology Command/9th Army Signal Command (NETCOM/9th ASC) and the RCIO-Europe to ensure the Army in Europe can complete the transition to IPv6 before fiscal year 2008.

E-7. SERVER POLICY

NOTE: This paragraph supplements guidance to AR 25-1, paragraphs 6-2b(3), 6-2c, 6-2d, 6-3, and 6-4n, which all organizations are responsible for following. The POC for information in this paragraph is the USAREUR G6 (AEAIM-T, DSN 370-9960).

a. Server Acquisition. Organizations in the Army in Europe will not purchase servers without express written approval from the USAREUR G6 or the RCIO-Europe.

b. Server Connectivity and Accreditation.

(1) Before an organization connects a server to the Army in Europe network, the server must be certified and accredited. A certification agent appointed by a DAA will conduct certification testing on the server. Certification testing is required to ensure that the Army in Europe computer security baseline, service packs, critical updates, and all identified information assurance vulnerability alert (IAVA) actions have been applied to the server. Test results must be included in the organization's SSAA and provided to the DAA for acceptance of residual risks and formal approval to connect to the network. The USAREUR IAPM and supporting NSCs can provide technical assistance on certification testing and the accreditation process.

(2) No server will be connected or reconnected to the Army in Europe network or reutilized without complying with (1) above. If a server must be connected to meet urgent operational warfighting requirements, the server will be registered as soon as possible after being connected.

(3) No Army in Europe organization may activate a Microsoft Exchange 2000 or newer server without—

(a) Coordination with the USAREUR G6 (Task Force Enterprise and CTO offices) and the 5th Signal Command G7.

(b) Approval from the Windows Active Directory (AD) Configuration Control Board, 5th Signal Command.

(4) Organizations that have hardware systems not capable of operating in the Windows 2000 environment must replace those systems or operate them in a stand-alone configuration (not connected to the Army in Europe network). If an organization determines that a pre-Windows 2000 operating system is required to perform its mission, it must submit a request for an exception to policy that fully justifies why the old operating system must remain in use and the expected timeline to complete upgrading it to the current baseline operating system.

c. Policy and Architectural Compliance. After a server is connected to the Army in Europe network, the Information Infrastructure Assessment Team will make periodic inspections to ensure that regulatory guidelines are followed. In addition, the Regional Computer Emergency Response Team, Europe (RCERT-E), will periodically conduct random network scans to verify server compliance.

E-8. E-MAIL POLICY

NOTE: This paragraph supplements guidance to AR 25-1, paragraph 6-4m, which all organizations are responsible for following.

Supplemental policy on e-mail in the Army in Europe is at *https://www.us.army.mil/suite/folder/1047603*. (**NOTE:** Persons who have not previously been granted access to the page will have to request access before they will be able to view any documents.)

E-9. METADATA TAGGING

NOTE: This paragraph supplements guidance to AR 25-1, paragraph 4-8, which all organizations are responsible for following.

The Army in Europe Unclassified Metadata Tagging Program prescribes policy and procedures to identify and manage documents for the purpose of "detection" through a consistent and flexible search. The USAREUR metadata standard (UMS) specifies a set of information fields that are to be used to describe any data or service asset that is on an Army in Europe network. Army in Europe record managers will ensure that the UMS is used consistently across the disciplines, domains, and data formats in the European theater. Implementation guidance is at *https://www.us.army.mil/suite/folder/1047603*. (**NOTE:** Persons who have not previously been granted access to the page will have to request access before they will be able to view any documents.)

E-10. TELECOMMUNICATIONS

NOTE: This paragraph supplements guidance to AR 25-1, paragraphs 6-4 and 6-5, which all organizations are responsible for following.

Implementation guidance for telecommunications is at *https://www.us.army.mil/suite/folder/942653*. (**NOTE:** Persons who have not previously been granted access to the page will have to request access before they will be able to view any documents.) Documentation on the website covers—

a. Cell phones (supplements AR 25-1, para 6-4w).

b. Commercial-usage requirements (supplements AR 25-1, paras 6-1 and 6-4).

c. Defense Red Switch Network (supplements AR 25-1, para 6-5b(1)).

d. DSN (supplements AR 25-1, para 6-5b).

e. DSN Usage and Base Communications Ordering System (DUBOS) (supplements AR 25-1, para 6-5b).

f. Integrated service digital network (ISDN) and Defense Information Systems Network requirements (supplements AR 25-1, para 6-5a).

g. Local service requests (supplements AR 25-1, para 6-4c).

h. Long-haul requirements (supplements AR 25-1, para 6-5).

i. Telephone Control Officer Program (supplements AR 25-1, para 6-4e(3)).

E-11. SPECTRUM MANAGEMENT

NOTE: This paragraph supplements guidance to AR 25-1, paragraph 6-4bb, which all organizations are responsible for following.

Implementation guidance for spectrum management is at *https://www.us.army.mil/suite/folder/1047603*. (**NOTE:** Persons who have not previously been granted access to the page will have to request access before they will be able to view any documents.)

E-12. DEFENSE MESSAGE SYSTEM

When using the Defense Message System (DMS), all Army in Europe organizations will follow the guidance in AR 25-1, paragraph 6-5f, as supplemented by the DMS guidance at *https://www.us.army.mil/suite/folder/1047603*. (**NOTE:** Persons who have not previously been granted access to the page will have to request access before they will be able to view any documents.)